



SPYWOLF

Security Audit Report



Completed on
September 6, 2022

MADE IN USA 

 @SPYWOLFNETWORK

 @SPYWOLFNETWORK

 SPYWOLF.CO



OVERVIEW

This audit has been prepared for **STFU Labs** to review the main aspects of the project to help investors make an informative decision during their research process.

You will find a summarized review of the following key points:

- ✓ Contract's source code
- ✓ Owners' wallets
- ✓ Tokenomics
- ✓ Team transparency and goals
- ✓ Website's age, code, security and UX
- ✓ Whitepaper and roadmap
- ✓ Social media & online presence

“

The results of this audit are purely based on the team's evaluation and does not guarantee nor reflect the projects outcome and goal

- SPYWOLF Team -

”

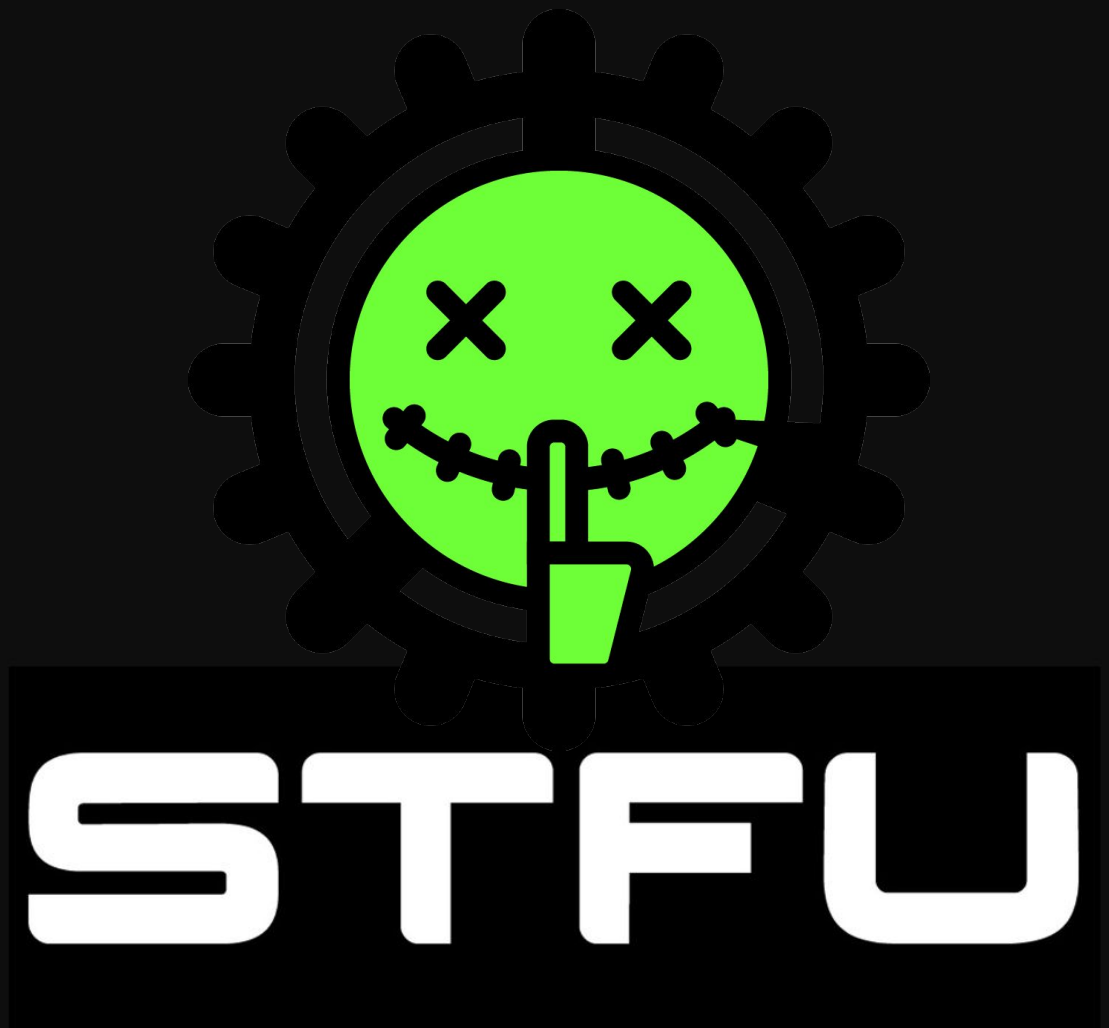




TABLE OF CONTENTS

Project Description	01
Contract Information	02
Current Stats	03-04
Featured Wallets	05
Vulnerability Check	06
Threat Levels	07
Found Threats	08
Good Practices	09
Tokenomics	10
Team Information	11
Website Analysis	12
Social Media & Online Presence	13
About SPYWOLF	14
Disclaimer	15





PROJECT DESCRIPTION

According to their website:

Users will be able to use telegram to do an old-school style, double-or-nothing coin flip game with their \$STFU tokens.

Release Date: Presale starts on August, 2022

Category: Gamble



CONTRACT INFO

Token Name
STFU Labs

Symbol
STFU

Contract Address

0xb65D39214dCe3691346Fe16482C5Ff81cbdf177D

Network

Binance Smart Chain

Language

Solidity

Deployment Date

Sept 04, 2022

Verified?

Yes

Total Supply

100,000

Status

Not launched

TAXES

Buy Tax

11%

Sell Tax

11%

*Taxes can be changed in future



Our Contract Review Process

The contract review process pays special attention to the following:

- ✓ Testing the smart contracts against both common and uncommon vulnerabilities
- ✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
- ✓ Ensuring contract logic meets the specifications and intentions of the client.
- ✓ Cross referencing contract structure and implementation against similar smart contracts produced by industry leaders.
- ✓ Thorough line-by-line manual review of the entire codebase by industry experts.

Blockchain security tools used:

- OpenZeppelin
- Mythril
- Solidity Compiler
- Hardhat



CURRENT STATS

(As of Sept 06, 2022)



Liquidity

Not added yet



Burn

No burnt tokens

Status:
Not Launched!

MaxSellTxAmount
500

DEX:
PancakeSwap

LP Address(es)

Liquidity not added yet



TOKEN TRANSFERS STATS

Transfer Count	1
Uniq Senders	1
Uniq Receivers	1
Total Amount	99999.999999999999 STFU
Median Transfer Amount	99999.999999999999 STFU
Average Transfer Amount	99999.999999999999 STFU
First transfer date	2022-09-04
Last transfer date	2022-09-04
Days token transferred	1

SMART CONTRACT STATS

Calls Count	1
External calls	1
Internal calls	0
Transactions count	1
Uniq Callers	1
Days contract called	1
Last transaction time	2022-09-04 15:37:13 UTC
Created	2022-09-04 15:37:13 UTC
Create TX	0x6a10b32ebe66ddc788e6209c3a3bf9941a0f97a78510aee2fc78dfb2518b84eb
Creator	0x564ee7ad6f85cee09403907c975fda191d52121f



FEATURED WALLETS

Owner address	0x564ee7ad6f85cee09403907c975fda191d52121f
LP address	Liquidity not added yet

TOP 3 UNLOCKED WALLETS

1



Same as owner

*Tokens are not distributed yet



VULNERABILITY CHECK

Design Logic	Passed
Compiler warnings.	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed



THREAT LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Low Risk

Issues on this level are minor details and warning that can remain unfixed.

Informational

Information level is to offer suggestions for improvement of efficacy or security for features with a risk free factor.



FOUND THREATS

⚠ High Risk

Owner can change reward pool to any address and transfer the tokens from previous reward pool to the new reward pool.

```
function setRewardPool(address newRewardPool) external onlyOwner {
    require(newRewardPool != address(0),
        "Call renounceOwnership to transfer owner to the zero address.");
    require(newRewardPool != BURN_ADDRESS,
        "Call renounceOwnership to transfer owner to the zero address.");
    address previousRewardPool = rewardPool;
    setExcludedFromFee(rewardPool, false);
    setExcludedFromFee(newRewardPool, true);
    setExcludedFromReward(newRewardPool, true);

    _allowances[rewardPool][newRewardPool] = balanceOf(rewardPool);
    if(balanceOf(rewardPool) > 0) {
        _transfer(rewardPool, newRewardPool, balanceOf(rewardPool));
    }

    rewardPool = newRewardPool;
    emit NewRewardPoolSet(previousRewardPool, newRewardPool);
}
```



FOUND THREATS

⚠ High Risk

Owner can mint (create) new tokens to the rewardPool address. This can lead to token's price inflation.

```
function replenishRewards( uint256 amount) external onlyOwner {
    require(amount <= _tTotal, "amount cannot be more than supply");

    uint256 rAmount = amount * _getRate();

    _tTotal += amount;
    _rTotal += rAmount;

    if(!_isExcluded[rewardPool]){
        _tOwned[rewardPool] += amount;
    }

    _rOwned[rewardPool] += rAmount;

    emit Transfer(address(0), rewardPool, amount);
}
```



FOUND THREATS

Medium Risk

Owner can change buy, sell and transfer fees up to 20% each.
Buy and sell combined = 40%.

```
uint256 constant public MAX_TAX = 2000;

function setTaxesBuy(uint16 liquidityFee, uint16 reflectionFee,
    uint16 marketingFee, uint16 burnFee) external onlyOwner {
    uint16 totalTax = liquidityFee + reflectionFee + marketingFee + burnFee;
    require(totalTax <= MAX_TAX);
    _buyFees = Fees(reflectionFee, liquidityFee, marketingFee, burnFee, totalTax);
}

function setTaxesSell(uint16 liquidityFee, uint16 reflectionFee,
    uint16 marketingFee, uint16 burnFee) external onlyOwner {
    uint16 totalTax = liquidityFee + reflectionFee + marketingFee + burnFee;
    require(totalTax <= MAX_TAX);
    _sellFees = Fees(reflectionFee, liquidityFee, marketingFee, burnFee, totalTax);
}

function setTaxesTransfer(uint16 liquidityFee, uint16 reflectionFee,
    uint16 marketingFee, uint16 burnFee) external onlyOwner {
    uint16 totalTax = liquidityFee + reflectionFee + marketingFee + burnFee;
    require(totalTax <= MAX_TAX);
    _transferFees = Fees(reflectionFee, liquidityFee, marketingFee, burnFee, totalTax);
}
```

- Recommendation:
 - Considered as good tax deduction practice is buy and sell fees combined not to exceed 25%.



Informational

Owner can set change max transaction amount but can't lower it than 0.1% of total supply.

```
function setMaxTxPercents(uint256 buyPercent, uint256 buyDivisor,
uint256 sellPercent, uint256 sellDivisor) external onlyOwner() {
    _buyMaxTxAmount = (_tTotal * buyPercent) / buyDivisor;
    buyMaxTxAmountUI = (INITIAL_SUPPLY * buyPercent) / buyDivisor;
    _sellMaxTxAmount = (_tTotal * sellPercent) / sellDivisor;
    sellMaxTxAmountUI = (INITIAL_SUPPLY * sellPercent) / sellDivisor;
    require(_sellMaxTxAmount >= (_tTotal / 1000) && _buyMaxTxAmount >= (_tTotal / 1000),
    "Max Transaction amts must be above 0.1% of total supply.");
}
```

Owner can exclude address from transaction fees and limits.

```
function setExcludeAll(address account, bool enabled) external onlyOwner {
    setExcludedFromFee(account, enabled);
    setExcludedFromReward(account, enabled);
    setExcludeFromLimits(account, enabled);
}
```



RECOMMENDATIONS FOR

GOOD PRACTICES

1

Consider fundamental tradeoffs

2

Be attentive to blockchain properties

3

Ensure careful rollouts

4

Keep contracts simple

5

Stay up to date and track development

STFU Labs

GOOD PRACTICES FOUND

- ✓ The owner cannot stop or pause the contract
- ✓ The owner can set a transaction limit, but can't lower it than 0.1% of total supply



⚠ There is no information about the initial tokens distribution in project's website and/or social media pages.

TOKENOMICS



THE TEAM

! The team is
anonymous

KYC INFORMATION

! No KYC

We recommend the team to get a KYC in order to ensure trust and transparency within the community.





WEBSITE

Website URL

<https://stfulabs.com/>

Domain Registry

<https://www.godaddy.com>

Domain Expiration

Expires on 2023-09-02

Technical SEO Test

Passed

Security Test

Passed. SSL certificate present

Design

Single page design,
appropriate color scheme.

Content

⚠ Content's text is
overlapping and very hard
to read.

Whitepaper

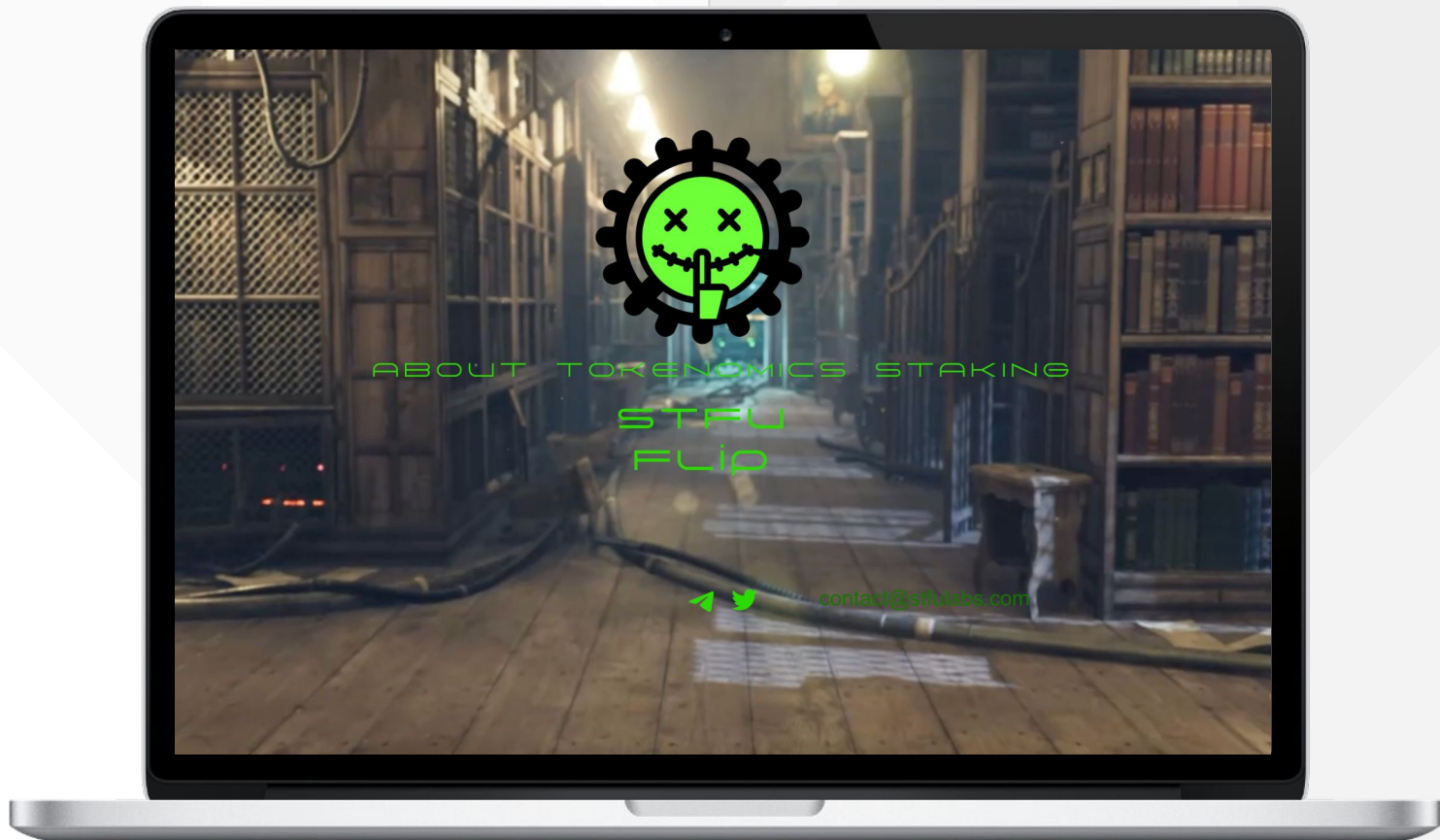
⚠ No whitepaper.

Roadmap

⚠ No

Mobile-friendly?

No



stfulabs.com

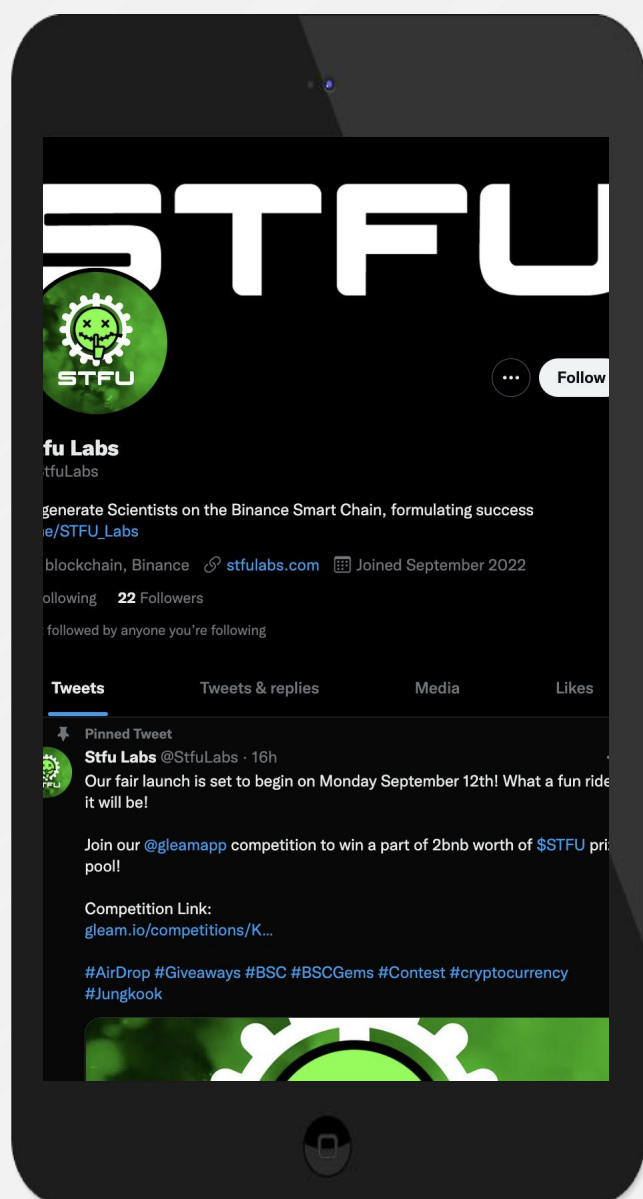


SOCIAL MEDIA & ONLINE PRESENCE



ANALYSIS

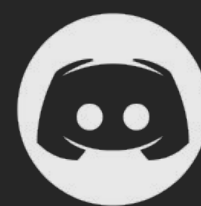
Project's social media pages are active with organic users



Twitter

@STFULabs

- 22 followers
- 3 total posts, posts every day
- New account



Discord

- Not available



Telegram

@stfu_labs

- 289 members
- Active members
- Active mods



Medium

- Not available



SPYWOLF

CRYPTO SECURITY

Audits | KYCs | dApps
Contract Development

ABOUT US

We are a growing crypto security agency offering audits, KYCs and consulting services for some of the top names in the crypto industry.

- ✓ OVER 150 SUCCESSFUL CLIENTS
- ✓ MORE THAN 500 SCAMS EXPOSED
- ✓ MILLIONS SAVED IN POTENTIAL FRAUD
- ✓ PARTNERSHIPS WITH TOP LAUNCHPADS, INFLUENCERS AND CRYPTO PROJECTS
- ✓ CONSTANTLY BUILDING TOOLS TO HELP INVESTORS DO BETTER RESEARCH

To hire us, reach out to
contact@spywolf.co or
t.me/joe_SpyWolf

FIND US ONLINE



SPYWOLF.CO



SPYWOLF.NETWORK



@SPYWOLFNETWORK



@SPYWOLFOFFICIAL



@SPYWOLFNETWORK



@SPYWOLFNETWORK



Disclaimer

This report shows findings based on our limited project analysis, following good industry practice from the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, overall social media and website presence and team transparency details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report.

While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER:

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

No one shall have any right to rely on the report or its contents, and SpyWolf and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (SpyWolf) owe no duty of care towards you or any other person, nor does SpyWolf make any warranty or representation to any person on the accuracy or completeness of the report.

The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and SpyWolf hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, SpyWolf hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against SpyWolf, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report. The analysis of the security is purely based on the smart contracts, website, social media and team.

No applications were reviewed for security. No product code has been reviewed.